Információbiztonsági előírások
szerződéses partnerek részére

INFORMÁCIÓBIZTONSÁGI ELŐÍRÁSOK SZERZŐDÉSES PARTNEREK RÉSZÉRE

Információbiztonsági előírások
szerződéses partnerek részére

Tartalomjegyzék

Információbiztonsági előírások szerződéses partnerek részére

1. Cél

A jelen dokumentum a Telenor adatait elérő, létrehozó, tároló vagy feldolgozó és/vagy a Telenor információs eszközeit használó felhasználókra vonatkozó alapvető előírásokat tartalmazza. A dokumentum célja a felhasználók által betartandó legfontosabb információbiztonsági szabályok meghatározása.

2. Hatály

A jelen dokumentum földrajzi korlátozás nélkül a Telenor információs eszközeihez hozzáférő valamennyi felhasználóra érvényes.

3. Kivételek

A Telenor egyes egységeire vagy területeire, illetve a Telenor egyes információs eszközeire más szabályzatok, irányelvek, jogszabályok és utasítások vonatkozhatnak. Az információs eszköz vagy informatikai erőforrás felelősének, illetve más jogosult személynek a feladata, hogy az egyes felhasználókat az ilyen kivételekről tájékoztassa.

4. Alapvető előírások a felhasználók részére

4.1 A Telenor információs eszközeinek megengedett használata

A Telenor információs eszközei nem használhatók fel a Telenor Szállítói Etikai Elvekkel, a titoktartási kötelezettséggel vagy a szerződéssel ellentétes módon.

A Telenor információs eszközeinek jogosulatlan felhasználása vagy az erre irányuló kísérlet szigorúan tilos. Ez a Telenor információihoz való jogosulatlan hozzáférésre, valamint az információk manipulációjára és/vagy terjesztésére is vonatkozik. **A felhasználók azonosítására szolgáló adatok (pl. felhasználónév, jelszó, PIN-kód) más felhasználók részére való átadása vagy más felhasználók ilyen adatainak felhasználása vagy ennek megkísérlése szigorúan tilos és a szerződéses jogviszonyt érintő szankciókat von maga után.**

4.2 Adatkezelés

A Telenor informatikai erőforrásai az üzleti információk tárolására, továbbítására, feldolgozására és használatára szolgálnak. Az informatikai erőforrások minden egyéb felhasználása (pl. személyes használat) korlátozott, és nem járhat üzleti célt szolgáló erőforrások rendelkezésre állásának veszélyeztetésével. A szerződéses partnerek felhasználói privát adatokat a Telenor által rendelkezésre bocsátott eszközökön nem tárolhatnak.

Az üzleti adatok nem Telenorhoz tartozó informatikai erőforráson (a Telenor irányításán kívül eső külső feleknél) kizárólag az adatok/eszközök felelőseinek előzetes, írásos hozzájárulásával, megfelelő védelmi mechanizmus alkalmazása mellett továbbíthatók, dolgozhatók fel és/vagy tárolhatók.

Adatgyűjtési-, és rendszerezési tevékenység csak a Felek között létrejött egyéb szerződésekben tett kifejezett felhatalmazás mellett végezhető.

5. Hozzáférés-védelem

5.1 A hozzáférési adatokra vonatkozó előírások

A hozzáférési jogosultságok a Telenor információs eszközeinek – ideértve többek közt az informatikai infrastruktúrát, az informatikai erőforrásokat és az adatokat – védelmére szolgálnak.

A hozzáférésre szolgáló felhasználói adatokat, például a PIN-kódokat, jelszavakat, tanúsítványokat, tokeneket, azonosító-kártyákat és intelligens kártyákat kizárólag birtokosuk használhatja. A hozzáférési adatokat meg kell jegyezni vagy biztonságos helyen kell tárolni. A hozzáférési adatokat tilos továbbadni, megosztani, közzétenni vagy a felelősüktől eltérő személyek vagy szervezetek számára hozzáférhetővé tenni.

Ha a hozzáférést biztosító adatok titkossága sérül (mások számára ismertté válnak vagy elvesznek), akkor az ilyen adatokat lehetőség szerint haladéktalanul le kell tiltani, és mindenképpen újat kell helyettük választani. A hozzáférést biztosító adatokkal való visszaélés gyanúja esetén ezt azonnal jelenteni kell az információbiztonsági csoportnak (az elérhetőségi adatokat lásd az I. függelékben).

A Telenor információs eszközeihez hozzáférő valamennyi felhasználó egyéni felelőssége, hogy a hozzáférés-védelemre és a hozzáférési adatok használatára vonatkozó hatályos előírásokat ismerje és betartsa.

Az a személy, akinek hozzáférési adataival bármely erőforráshoz hozzáférnek, a hozzáférési adataival végrehajtott összes cselekedetért felelősségre vonható.

A különböző eszközök, így a számítógépek vagy a telefonok képernyőjét le kell zárni, amikor a felhasználó nem tudja felügyelni őket (pl. a számítógépeket az íróasztal elhagyása előtt zárolni kell, a mobiltelefonokat pedig PIN-védelemmel kell lezárni).

5.2 A jelszavakra vonatkozó különleges előírások

A Telenor informatikai erőforrásaira a következő jelszószabályzat vonatkozik:

- A jelszónak legalább 8 karakterből kell állnia
- A jelszó az alábbi négy csoport közül legalább háromból kell, hogy karaktereket tartalmazzon:
    - Nagybetűk
    - Kisbetűk
    - Numerikus karakterek
    - Speciális karakterek
- A jelszó nem tartalmazhat olyan triviális személyes azonosítókat, mint név, felhasználónév, becenév, születésnap stb.
- A Telenor informatikai erőforrásaihoz való hozzáférésre szolgáló jelszavak máshol nem használhatók.
- A jelszavakat 90 naponta meg kell változtatni még akkor is, ha ezt a rendszer nem kéri.
- Az új jelszó a korábbi 10 jelszó egyikével sem egyezhet meg.
- Jelszómódosítást követően az új jelszó 24 órán keresztül nem változtatható meg ismét.

Ha a rendszer nem követeli meg ezeket a beállításokat, a felhasználó köteles biztosítani, hogy a jelszavai megfeleljenek ezeknek a követelményeknek. A PIN-kódokkal kapcsolatos követelményeket a mobil eszközökre vonatkozó előírások (9. oldal) tartalmazzák.

5.3 Azonosító-kártyákra vonatkozó előírások

Minden olyan személy, aki ideiglenes vagy állandó, Telenor által biztosított azonosító-kártyát kap, beleértve a munkavállalókat, látogatókat, külső szolgáltatókat, tanácsadókat, szerviz- vagy más jogosult személyzetet, köteles jól látható módon viselni azonosító-kártyáját a Telenor épületeiben.

Az azonosító-kártya szigorúan személyre szóló, és kizárólag azt a személyt azonosítja, aki azt kapta. Az azonosító-kártyát más személynek átengedni szigorúan tilos. Amennyiben egy felhasználó szándékos magatartása vagy súlyos gondatlansága miatt illetéktelen személyek jutnak be a Telenor területeire, ez a szerződéses jogviszonyt érintő szankciókat vonhat maga után. Az azonosító-kártya elvesztése vagy ellopása esetén azonnal bejelentést kell tenni (az elérhetőségi adatokat lásd az I. függelékben).

Az azonosító-kártya átadása előtt a Telenor egy jogosult munkavállalója köteles ellenőrizni az illető személyazonosságát (pl. a személyi igazolvány segítségével).

Az ideiglenes (látogatói) azonosító-kártyát viselő személyeket ott-tartózkodásuk teljes időtartama alatt egy állandó belépési jogosultsággal rendelkező Telenor munkavállalónak kell kísérnie.

6. Az elektronikus üzenetküldésre vonatkozó előírások

Az elektronikus üzenetek elsősorban üzleti célokat szolgálnak. Az elektronikus üzenetek magáncélú felhasználását minimálisra kell korlátozni. Archiválási szempontból az elektronikus üzenetek normál levélnek minősülnek. Az elektronikus üzenetek csatolmányai az üzenet részének tekintendők.

A felhasználók nem küldhetnek és terjeszthetnek láncleveleket elektronikus üzenetek formájában, és nem továbbíthatnak más felhasználóktól vagy külső hálózatokból érkező sértő, levélszemétnek minősülő vagy kéretlen e-mail üzeneteket.

Az üzleti e-maileknek a nevet, beosztást és vállalatnevet tartalmazó aláírással kell végződnie. A privát e-mailek nem tartalmazhatnak olyan szöveget, amely összefüggésbe hozható a Telenorral, vagy amely olyan benyomást kelt, mintha az illető személy a Telenor véleményét közvetítené. A Telenor a megfelelőség ellenőrzése céljából vagy biztonsági okokból ellenőrizheti az e-mailek tartalmát, és ezt a külső felhasználók is elfogadják a Telenor részére küldött e-mailben (ez a Telenor webhelyén is fel van tüntetve).

Nyilvános vagy külső e-mailszolgáltatást tilos üzleti célra használni.

A Telenor Szállítói Etikai Elvekkel és/vagy az irányadó jogszabályokkal és előírásokkal ellentétes tartalmak nem terjeszthetők a vállalaton belül vagy azon kívül a Telenor informatikai erőforrásainak igénybevételével. Ilyen tartalomnak minősülnek egyebek mellett a pornográf, sértő, rasszista és más diszkriminatív anyagok.

A tulajdonjogi és/vagy szerzői jogi oltalom alá eső, a Telenor által fel nem használható információkat tartalmazó elektronikus üzeneteket törölni kell.

A külső címekre küldött, bizalmas információkat tartalmazó e-maileket és csatolmányaikat titkosítani kell, és a titkosításhoz kapcsolódó jelszavakat más csatornán kell továbbítani (pl. SMS-ben, személyesen). Az elektronikus üzeneteket a jelen dokumentumban leírtakkal és a Telenor egyéb vonatkozó előírásaival összhangban kell tárolni.

Azokat az adatokat, amelyek üzleti célokra már nem szükségesek és így a jogszabályi előírások szerint már nem tárolhatóak, a felhasználóknak törölniük kell. A felhasználók kötelesek postafiókjukat úgy strukturálni, hogy lehetővé tegyék az ilyen e-mailek törlését.

Amennyiben növelni kell a postafiók tárhelyének méretét, a felhasználónak meg kell indokolnia ennek üzleti szükségszerűségét, az illetékes rendszer üzemeltető pedig ellenőrizheti ezt.

Telenoros e-mail cím nem adható meg privát célú előfizetésekhez (például levelező listák). A Telenor nem vállal felelősséget az ilyen előfizetések megszűnéséből vagy az ilyen jellegű üzenetek kézbesítésének elmaradásából származó kárért/pénzügyi veszteségért.

Tilos levélszemétnek minősülő üzeneteket küldeni a Telenor informatikai erőforrásainak igénybevételével.

A Telenor jogosult a külső címre küldött üzenetek végére felelősségkizáró vagy más jogi nyilatkozatot helyezni. Az ilyen felelősségkizáró nyilatkozatok leszögezhetik, hogy az üzenetben kifejtett magánvélemények eltérhetnek a Telenor hivatalos álláspontjától vagy politikájától.

7. Az internethasználatra vonatkozó előírások

A Telenor által biztosított internet elérés elsősorban üzleti célra használandó, magáncélú felhasználásra csak korlátozottan vehető igénybe.

A Telenor Szállítói Etikai Elvekkel és/vagy az irányadó jogszabályokkal és előírásokkal ellentétes tartalmak, adatok, információk vagy internetes szolgáltatások nem tölthetők le, látogathatók, használhatók fel vagy tekinthetők meg a Telenor informatikai erőforrásainak igénybe vételével. Ilyen tartalomnak minősülnek egyebek mellett a pornográf, sértő, rasszista és más diszkriminatív anyagok.

Tilos a jogosulatlan, a Telenor előírásainak meg nem felelő szoftverek, futtatható kódok és/vagy (rosszindulatúnak tekinthető) programok letöltése (és futtatása). Minden letöltött tartalmat víruskereső programmal ellenőrizni kell.

A peer-to-peer fájl cserélő hálózatokhoz való csatlakozás és azok használata szigorúan tilos, amely szabály alól csak kifejezett üzleti indok esetében adhat felmentést az Információbiztonsági csoport.

A Telenor által biztosított internet-hozzáférést támadó vagy illegális tevékenységekre használni szigorúan tilos. Az erre irányuló kísérletek bejelentésre kerülnek az illetékes hatóságnál.

Az interneten keresztüli privát közlések nem tartalmazhatnak olyan információkat, amelyek összefüggésbe hozhatók a Telenorral, vagy amelyek olyan benyomást keltenek, mintha az illető személy a Telenor véleményét közvetítené.

A Telenor jogosult a felhasználók előzetes értesítése nélkül szűrni, letiltani és/vagy korlátozni az interneten elérhető információkhoz, webhelyekhez és szolgáltatásokhoz való hozzáférést.

8. Mobileszközökre és informatikai erőforrásokra vonatkozó előírások

Az üzleti adatok tárolására szolgáló valamennyi mobileszköz és informatikai erőforrás védelmét a következő módon kell biztosítani:

- Az eszközökben található tárolót titkosítani kell annak érdekében, hogy az eszközök elvesztése vagy ellopása esetén az adatok ne kerüljenek jogosulatlan kézbe.
- Az eszközöket minimum jelszavas/PIN-kódos védelemmel kell ellátni. Hordozható számítógépek és hasonló eszközök esetén a normál bejelentkezési eljárást kell alkalmazni. A kézi eszközöket minimum PIN-kódos védelemmel kell ellátni, és a PIN-kódnak legalább négy számjegyből kell állnia.
- A hordozható számítógépeket és kézi eszközöket meghatározott ideig tartó inaktivitás esetén automatikusan zárolni kell.
- Mobiltelefonok esetén 10 sikertelen feloldási kísérlet után az eszköznek automatikusan vissza kell állnia a gyári alapbeállításokra az összes tárolt adat törlésével.

- Ha az eszköz éjszakára a Telenor helyiségeiben marad, a felhasználó saját szekrényébe kell zárni. A Telenor üzleti helyiségein kívül is biztosítani kell az eszköz megfelelő védelmét (látható helyen nem szabad gépkocsiban hagyni).
- A mobil eszközt WiFi hozzáférési pontként használó felhasználók kötelesek megfelelő biztonsági mechanizmusokat alkalmazni a más eszközökkel és/vagy hálózatokkal történő kommunikáció védelméhez (titkosításához). (pl. WPA2-védelem engedélyezése).
- Nem megengedett az olyan mobileszközök és hozzáférési adatok megosztása, amelyek révén a Telenor informatikai erőforrásai, infrastruktúrája és adatai hozzáférhetővé válnak.
- A mobileszközöknek a Telenor mobil rádiós hálózatán keresztüli magáncélú használata minimálisra korlátozandó. A használat során nem terhelhetik a Telenor ügyfeleinek történő magas színvonalú szolgáltatás nyújtásához szükséges erőforrásokat. A Telenor informatikai erőforrásaihoz csatlakozó, de nem a Telenor irányítása alá tartozó eszközök használatát az Információbiztonságnak kell engedélyeznie (II. függelék). Ennek menetét külön előírás ismerteti. A Telenor előzetes jóváhagyása nélkül tilos az üzleti információk ilyen eszközökre történő másolása vagy mentése.
- Az informatikai erőforrások és/vagy adatok ellopását/elvesztését haladéktalanul be kell jelenteni a II. függelékben megadott címeken/telefonszámokon. Lopás esetén az ügyet jelenteni kell a rendőrségen, és a Telenorhoz el kell juttatni a vonatkozó rendőrségi jegyzőkönyvet. Amennyiben a Telenor illetékes részlegei azt állapítják meg, hogy az informatikai erőforrás ellopása/elvesztése a felhasználó gondatlanságának tudható be, a felhasználó köteles megtéríteni az ellopott/elvesztett berendezés teljes értékét.

9. A szoftverekre és licencekre vonatkozó előírások

A Telenornak minden szoftvert engedélyeznie kell, mielőtt azokat a végfelhasználók igénybe vehetik. Az engedélyezés azt jelenti, hogy a felelős személyzet (a műszaki, jogi és információbiztonsági részlegektől) ellenőrzi, hogy a Telenor környezetében hibamentesen működik-e a szoftver, valamint hogy a Telenor megállapodás vagy szerződés alapján rendelkezik-e érvényes licenccel.

Minden eszközt előre be kell állítani funkciójának megfelelően. Telenor tulajdonú eszközökre kizárólag az üzleti tevékenységekhez szükséges szoftverek telepíthetők. Az üzleti tevékenységekhez nem szükséges szoftvereket el kell távolítani, illetve jóvá kell hagyatni az arra jogosult személyzettel (szerződéses partner belső,vezetői szintű kapcsolattartója és Információbiztonság (II. függelék)). Az eredeti beállítást kizárólag a jogosult személyzet módosíthatja.

A szoftvereket kizárólag a jogosult személyzet telepítheti a Telenor tulajdonát képező eszközökre. A nem engedélyezett és illegális szoftvereket előzetes figyelmeztetés nélkül el kell távolítani. Nem engedélyezett szoftverek telepítése szigorúan tilos. Az illegális szoftverek telepítése szankcionálható.

A szoftverek jogosulatlan másolása nem megengedett.

10.A megfelelőség ellenőrzése

A Telenor információs eszközein belüli tevékenységről utólagosan megállapítható, hogy az mely felhasználóhoz tartozik. Minden informatikai erőforrás monitorozható, és valamennyi jogosult és jogosulatlan hozzáférési kísérlet naplózható. Ez elsősorban adminisztratív célt szolgál a Telenor információbiztonsági előírásainak (bizalmasság, sértetlenség és rendelkezésre állás) teljesítése, illetve a biztonsági előírások megszegésének felderítése érdekében.

A Telenor jogosult elektronikusan ellenőrizni minden elküldött és fogadott üzenetet a csalások, rosszindulatú programok, nem kívánatos vagy kártékony tartalmak felderítése érdekében a Telenor informatikai erőforrásainak igénybevételével elküldött üzenet privát vagy üzleti jellegétől függetlenül.

A Telenor informatikai erőforrásainak ellenőrzésére a licencek megszámlálása, a nem engedélyezett szoftverek, a felesleges tartalmak, a nemkívánatos futtatható kódok/rosszindulatú szoftverek és a Telenor előírásaival vagy a Szállítói Etikai Elvekkel össze nem egyeztethető egyéb tartalmak felismerése céljából kerülhet sor. Az ellenőrzések előtt nem szükséges előzetes figyelmeztetés kiadása. Az információk és/vagy informatikai erőforrások védelme érdekében a Telenor figyelmeztetés nélkül törölhet bármely fájlt, szoftvert vagy tartalmat. A Telenor jogosult ellenőrizni az informatikai erőforrásaihoz kapcsolódó bármely eszközön történő szoftverhasználatot. Az illegális szoftverek bármikor, előzetes figyelmeztetés nélkül eltávolíthatók.

A rendszerek és hálózatok biztonsági tesztelése nem megengedett. A biztonsági mechanizmusok felderítésére, visszafejtésére, meggyengítésére, kikapcsolására, kikerülésére vagy megsemmisítésére tett kísérletek az Információbiztonság engedélye nélkül nem végezhetőek.

A Telenor informatikai erőforrásaiban előforduló rendellenességeket, a rosszindulatú programok okozta támadások gyanúját, a berendezések és/vagy adatok ellopását, valamint a felhasználói hozzáférési adatok tárolására szolgáló egységek elvesztését vagy sérülését haladéktalanul jelenteni kell az Információbiztonságnak. A csalást és egyéb bűncselekményeket a Telenor belső vezetői szintű kapcsolattartójának is jelenteni kell.

Kivételes esetben a Telenor saját erőforrásain szükség szerint feltörheti, megváltoztathatja vagy kikerülheti a jelszavas védelmet az üzleti információk megszerzése, illetve a jogosulatlan vagy illegális cselekmények megakadályozása céljából.

11. Az előírások megszegésének következményei

A jelen előírások megszegése akár a jogosultságok visszavonását vagy a szerződéses kapcsolat megszűntetését is maga után vonhatja.

Az érintett felhasználókat vagy szerződéses partnereket pénzügyi/anyagi kártérítési kötelezettség is terhelheti.

A jelen előírások betartására kötelezett összes egyén köteles ismerni és mindenkor betartani ezeket, illetve a Telenor információs eszközeire vonatkozó egyéb előírásokat.

12. Fogalom-meghatározások

Jogosult személyzet

Az egyes információs eszközökhöz és/vagy informatikai erőforrásokhoz történő hozzáférésre jogosult személyzet. A jogosultság biztosítása dokumentált eljárás szerint történik. Jogosult személyzetnek minősülhetnek továbbá a személyzet azon tagjai, akik engedélyezési hatáskörrel rendelkeznek bizonyos területeken, így egyebek közt a hozzáférési jogok, módosítások, fejlesztések, beszerzések, szoftvercsomagok használata, eszközök használata stb. tekintetében.

Engedélyezett szoftver

A Telenor jogosult személyzete vagy az Információbiztonság által jóváhagyott szoftver, amelynek a használatára a Telenor érvényes licenccel rendelkezik.

Mobileszköz

Információbiztonsági előírások
szerződéses partnerek részére

Bármely olyan eszköz, amely a Telenor által irányított környezeten kívül is használható, ideértve többek közt a „handheld” eszközöket, mobiltelefonokat, laptopokat, táblagépeket stb.

Információs eszköz

Az információs eszközök körébe tartozik minden szoftver- és hardver az azokon tárolt adatokkal együtt, így egyebek mellett a fix és hordozható informatikai berendezések, kézi eszközök, információs rendszerek, hálózatok és bármely egyéb olyan informatikai infrastruktúra vagy szolgáltatás, amely az adatok tárolására, feldolgozására, létrehozására vagy kezelésére szolgál.

Informatikai erőforrások

Az informatikai erőforrások körébe tartozik minden szoftver- és hardvererőforrás, így egyebek mellett a helyhez kötött és hordozható informatikai berendezések, „handheld” eszközök, információs rendszerek, hálózatok és bármely más olyan informatikai infrastruktúra vagy szolgáltatás, amely az adatok tárolására, feldolgozására, létrehozására vagy kezelésére szolgál.

A Telenor helyiségei

A jelen dokumentum alkalmazásában a Telenor helyiségének minősül a Telenor által felügyelt, bérelt vagy a Telenor tulajdonában lévő összes épület, telephely, helyiség és terület.

Felelős

Olyan egyén vagy szervezeti egység, aki, vagy amely egy rendszer, folyamat vagy információ tekintetében átfogó felelősséggel tartozik. Ebben az összefüggésben tehát a „felelős” nem arra a személyre utal, aki ténylegesen rendelkezik az adott eszköz vagy erőforrás tulajdonjogával.

Privát információ

A felhasználók olyan magánjellegű adatai, például személyes fotói, videó- és hangfelvételei, dokumentumai, e-mail üzenetei stb., amelyek az illető Telenornál végzett szakmai tevékenységéhez nem köthető személyes információkat tartalmaznak, illetve amelynek használati engedélyével, vagy szerzői és/vagy tulajdonjogával a felhasználó rendelkezik.

Rosszindulatú program

Olyan kártékony szoftver, amely az adatok megsemmisítésére és/vagy kiszivárogtatására szolgál. A rosszindulatú programok közé tartoznak többek közt a vírusok, férgek, billentyűzetnaplózó alkalmazások stb.

Információbiztonsági előírások
szerződéses partnerek részére

Elektronikus üzenet

Az elektronikus üzenetek körébe tartoznak egyebek mellett az interneten keresztül vagy helyben továbbított e-mailek, az SMS (rövid szöveges üzenet), az MMS (multimédia-üzenet), az EDI (elektronikus adatcsere) és az azonnali üzenetküldés (pl. Skype).

Elektronikus üzenetküldő szolgáltatások

Elektronikus üzenetváltásra használt szolgáltatások.

Adathordozó

Az adatok tárolására alkalmas összes eszköz vagy eszközkomponens, mint például a CD, a DVD, a hordozható vagy rögzített merevlemez, a SIM-kártya és más, azonos vagy hasonló funkciót ellátó technológiák, illetve olyan eszközök, amelyeknek valamely beépített alkatrésze azonos vagy hasonló célra szolgál, például PDA, mobiltelefon stb.

Szórakoztató célú fájlok

Olyan fájlok, amelyek nem üzleti jellegű információkat, például szórakoztató jellegű zenei, videó-, kép- vagy szövegfájlokat tartalmaznak.

Levélszemét

Tömegesen kiküldött kéretlen üzenet.

Futtatható szoftvermodul

Olyan programobjektum (ActiveX-vezérlő, Java kisalkalmazás, Explorer-bővítmény stb.), amely kompatibilis böngészővel letölthető és futtatható. A rosszindulatú futtatható szoftvermodulok bármely olyan műveletet végre tudnak hajtani, amely a számítógépen található szoftverek vagy adatok sérüléséhez/károsodásához vezetnek.

Internet

Egymással összekapcsolt hálózatok globális rendszere, amely a szabványos internetprotokoll-készlet segítségével nyújt szolgáltatásokat és információkat.

Peer-to-peer (P2P)

Olyan alkalmazási réteg szintű virtuális számítógép-hálózat, amelyben minden számítógép egyszerre működik kliensként és a többi számítógépet kiszolgáló szerverként.

Felhasználó

Olyan személy, aki munkavállalóként, bérelt munkaerőként vagy az őt alkalmazó gazdaság társaság szerződéses jogviszonyban áll a Telenorral, és aki engedélyezett módon hozzáfér a Telenor információs eszközeihez.

Telenor

A Telenor a Telenor d.o.o. Serbia, a Telenor d.o.o. Montenegro, a Telenor Magyarország Zrt. és a Telenor Common Operation Zrt. vállalatokat (beleértve ezek összes fióktelepét) jelöli.

13. Függelékek

14.1 I. függelék

Az információbiztonság elérhetőségei:

- Telenor Magyarország: informationsecurity@telenor.hu
- Telenor Common Operations: information.security@telenor.rs

14.2 II. függelék

Értesítési címek, telefonszámok az információs eszközök vagy az azonosító-kártyák ellopása, elvesztése esetén:

- Telenor Magyarország: informationsecurity@telenor.hu, +36209302931
- Telenor Common Operations: information.security@telenor.rs